GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1923

En alianza con

TD SYNNEX FORTINET

BOLETIN DE CIBERINTELIGENCIA DE AMENAZAS

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	5		
MALWARE		4	
BRECHAS DE SEGURIDAD		1	
NOTICIAS DE CIBERSEGURIDAD			5
SECTOR GOBIERNO	1		

VULNERABILIDADES

CISA agrega siete vulnerabilidades explotadas conocidas al catálogo

CISA ha agregado siete nuevas vulnerabilidades a su Catálogo de Vulnerabilidades Explotadas Conocidas , con base en evidencia de explotación activa. En los productos afectados están, Ruckus, Red Hat, Linux, Jenkins, Oracle Java SE, apache Tomcat. Este tipo de vulnerabilidades son vectores de ataque frecuentes de los actores cibernéticos maliciosos y representan riesgos significativos para la empresa.

Prioridad: 1 Crítico.

Ampliar información:

- https://www.cisa.gov/news-events/alerts/2023/05/12/cisa-adds-seven-known-exploited-vulnerabilities-catalog

---

Hackean cuentas de correo electrónico de outlook con archivo de música .wav

El martes, Microsoft emitió un parche actualizado para abordar una vulnerabilidad que se había solucionado previamente en marzo, pero resultó ser ineficaz según investigadores de la comunidad de seguridad.

Prioridad: 1 Crítico.

Ampliar información:

- https://noticiasseguridad.com/seguridad-informatica/hackear-cuentas-de-correo-electronico-de-outlook-con-solo-un-archivo-de-musica-wav/

Vulnerabilidad permite privilegios de usuario root en Linux 6.3.1

El kernel de Linux es la parte más importante del sistema operativo Linux. Está a cargo de administrar los recursos del sistema, brindar los servicios necesarios y garantizar la estabilidad general del sistema. Como resultado, cualquier vulnerabilidad dentro del kernel tiene el potencial de generar implicaciones importantes, lo que podría poner en riesgo la seguridad e integridad general del sistema. Se ha descubierto que el kernel de Linux incluye una importante falla de seguridad, a la que se le ha asignado el identificador CVE-2023-32233.

Prioridad: 1 Crítico.

Ampliar información:

- https://noticiasseguridad.com/seguridad-informatica/obtenga-privilegios-de-usuario-root-en-linux-6-3-1-usando-esta-vulnerabilidad-con-este-codigo/

Vulnerabilidades críticas RCE y dos Zero-Days en parches de Microsoft lanzados en mayo

La actualización de seguridad de Microsoft para mayo de 2023 es la más ligera desde agosto de 2021 con correcciones para un total de 49 nuevas vulnerabilidades, incluidas dos que los atacantes han estado explotando activamente.
La actualización incluye correcciones para nueve vulnerabilidades en el motor Chromium en el que se basa el navegador Edge de Microsoft. La empresa identificó siete de las 40 vulnerabilidades restantes como de gravedad crítica y el resto como "importantes".

Prioridad: 1 Crítico.

Ampliar información:

- https://www.darkreading.com/vulnerabilities-threats/microsoft-patches-two-zero-day-vulnerabilities
- https://www.ciberseguridadlatam.com/2023/05/11/microsoft-parcheo-tres-errores-de-dia-cero-en-mayo/
- https://msrc.microsoft.com/update-guide/releaseNote/2023-May?ranMID=43674&ranEAID=FE4O7wtxe6g&ranSiteID=FE4O7wtxe6g-jEVg_aXi.vCsCVGnbVutpw&epi=FE4O7wtxe6g-jEVg_aXi.vCsCVGnbVutpw&irgwc=1&OCID=AID2200057_aff_7795_1243925&tduid=%28ir__sg223zle2wkfbkljuvcdk9mugv2x661hzfahaiv900%29%287795%29%281243925%29%28FE4O7wtxe6g-

jEVg_aXi.vCsCVGnbVutpw%29%28%29&irclickid=_sg223zle2wkfbkljuvcdk9mugv2x661hzfahaiv900

Vulnerabilidad de inyección de comando TP-Link Archer AX-21 (CVE-2023-1389) explotada en estado salvaje

Existe una vulnerabilidad de inyección de comandos en las versiones de firmware de TP-Link Archer AX21 (AX1800) anteriores a la 1.1.4 Build 20230219 que permite a un atacante no autenticado inyectar comandos y obtener acceso a la raíz a través de una solicitud POST. La vulnerabilidad tiene una puntuación base CVSS de 8,8 y tiene una calificación ALTA.

Prioridad: 1 Crítica.

Ampliar información:

- https://fortiguard.fortinet.com/threat-signal-report/5157
- https://www.tp-link.com/us/support/faq/3643/?wgu=296930_16644_16839220644585_4d054b6d09&wgexpiry=1715458064&source=webgains&siteid=16644

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y/o aplicaciones actualizadas.
- Realizar actualizaciones directamente desde fabricantes y/o desarrolladores oficiales.

- Emplear controles compensatorios si no se puede realizar la actualización inmediatamente, dichos controles pueden incluir controles tecnológicos y soluciones de seguridad avanzadas que le permitan minimizar el riesgo de que alguna vulnerabilidad sea explotada.
- Tener una política y un plan de mitigación de vulnerabilidades periódico.
- Contar con soluciones de gestión de vulnerabilidades que le permita hacer la priorización de estas.
- Adquirir tecnologías que le permitan bloquear accesos mal intencionados o intentos de explotación de vulnerabilidades conocidas y de día cero.
- Contar con servicios de Ethical Hacking para identificar posibles superficies de ciberataque antes de que lo hagan sus adversarios, protegiendo los datos sensibles de un uso indebido o de robo, ayudando a prevenir las amenazas en la seguridad de los datos e identificar las vulnerabilidades que pueden ir más allá del sistema perimetral, con el fin de establecer un análisis holístico de las amenazas que puedan comprometer la seguridad de los datos críticos de la compañía, entre otras.

MALWARE

Resumen de ransomware - Maorí

Cada dos semanas, FortiGuard Labs recopila datos sobre variantes de ransomware de interés que han estado ganando terreno dentro de los conjuntos de datos y la comunidad OSINT. El informe Ransomware Roundup tiene como objetivo brindar a los lectores información breve sobre el panorama en evolución del ransomware y las soluciones de Fortinet que protegen contra esas variantes.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.fortinet.com/blog/threat-research/ransomware-roundup-maori

Un nuevo troyano de suscripción infecta más de 600.000 dispositivos

Se debe tener precaución con un nuevo troyano que está infectando dispositivos móviles a través de la tienda oficial de aplicaciones de Google Play. Este troyano, llamado Fleckpe**,** se presenta como una aplicación legítima de edición de imágenes, pero en realidad es un software malicioso que puede provocar graves consecuencias, como el robo de información personal y financiera, la suscripción a servicios de pago sin consentimiento y la descarga de software malicioso.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.elcolombiano.com/tecnologia/troyano-fleckpe-infecto-620000-dispositivos-EB21311665
- https://latam.kaspersky.com/about/press-releases/2023_fleckpe-troyano-de-suscripcion-se-propaga-a-traves-de-apps-de-edicion-de-fotos-y-fondos-de-pantalla

RapperBot DDoS Botnet se expande al criptojacking

FortiGuard Labs ha encontrado nuevas muestras de la campaña RapperBot activa desde enero de 2023. RapperBot es una familia de malware que se dirige principalmente a dispositivos IoT. Además, informó sobre sus campañas anteriores en agosto de 2022 y diciembre de 2022, esas campañas se centraron en dispositivos de fuerza bruta con credenciales SSH o Telnet débiles o predeterminadas para expandir la huella de la botnet con el fin de lanzar ataques de denegación de servicio distribuido (DDoS).

Prioridad: 2 Urgente.

Ampliar información:

- https://www.fortinet.com/blog/threat-research/rapperbot-ddos-botnet-expands-into-cryptojacking

---

La APT norcoreana Kimsuky lanza una campaña mundial de spear phishing

El grupo APT patrocinado por el estado norcoreano conocido como Kimsuky ha sido observado utilizando un nuevo componente de malware llamado ReconShark.
Según un aviso publicado por los investigadores de seguridad de SentinelOne el jueves, ReconShark se distribuye a través de correos electrónicos dirigidos de spear-phishing, Los cuales contienen enlaces de OneDrive que conducen a la descarga de documentos y la activación de macros dañinas.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/
- https://www.ciberseguridadlatam.com/2023/05/10/la-apt-norcoreana-kimsuky-lanza-una-campana-mundial-de-spear-phishing/

Recomendaciones generales sobre Malware:

- Controlar de forma minuciosa las conexiones de acceso remoto a su infraestructura: prohíba las conexiones desde redes públicas, permita el acceso RDP solo mediante un canal VPN y use contraseñas seguras y únicas con la autenticación en dos pasos.
- Mantener actualizado el software crítico de manera oportuna, poniendo énfasis en el sistema operativo, las soluciones de seguridad, los clientes de VPN y las herramientas de acceso remoto.
- Mantener a sus empleados constantemente en capacitaciones de concientización de ciberseguridad y en programas de sensibilización de ciberseguridad. En Gamma Ingenieros contamos con un programa completo de sensibilización en ciberseguridad, para obtener más información contacte a su gerente de cuenta, preguntando por nuestro programa de sensibilización y nuestra plataforma propietaria, Gamma Cyberacademy ©.
- Emplear soluciones de ciberseguridad avanzadas para proteger los dispositivos de trabajo y el perímetro de la red corporativa.
- Mantener actualizadas sus soluciones de ciberseguridad.
- Descargar aplicaciones solo de fuentes de confianza, como la tienda oficial de aplicaciones de Google Play Store.
- Revisar las calificaciones y opiniones de otras personas antes de descargar cualquier aplicación, especialmente si es una aplicación bancaria o financiera.
- No responder a llamadas telefónicas de números desconocidos o sospechosos, especialmente si solicitan información personal o financiera.
- No compartir información personal o financiera a través del teléfono o correo electrónico, a menos que esté seguro de la identidad del destinatario.

BRECHAS DE SEGURIDAD

Intel investiga la fuga de claves privadas de Intel Boot Guard

Intel está investigando la filtración de supuestas claves privadas utilizadas por la función de seguridad Intel Boot Guard, lo que podría afectar su capacidad para bloquear la instalación de *firmware* UEFI malicioso en dispositivos MSI.
Intel Boot Guard es una característica de seguridad integrada en el hardware Intel moderno diseñado para evitar la carga de *firmware* malicioso, conocido como *bootkits* UEFI. Es una característica fundamental que se utiliza para cumplir con los requisitos de arranque seguro de UEFI de Windows.

Prioridad: 2 Urgente.

Ampliar información:

- https://www.bleepingcomputer.com/news/security/intel-investigating-leak-of-intel-boot-guard-private-keys-after-msi-breach/

NOTICIAS DE CIBERSEGURIDAD

Dragos bloquea un ataque de ransomware y descarta un intento de extorsión

Un grupo de ransomware ha intentado sin éxito extorsionar a Dragos, según ha confirmado la firma de ciberseguridad industrial el miércoles, y ha asegurado que ninguno de sus sistemas o su plataforma Dragos ha sido violado.

El grupo delictivo obtuvo acceso al comprometer la dirección de correo electrónico personal de un nuevo empleado de ventas antes de su fecha de inicio y, posteriormente, utilizó su información personal para hacerse pasar por el empleado de Dragos y realizar los pasos iniciales en el proceso de incorporación de empleados. El grupo accedió a los recursos que un nuevo empleado de ventas suele utilizar en SharePoint y en el sistema de gestión de contratos de Dragos.

Prioridad: 3 Importante.

Ampliar información:

- https://twitter.com/vxunderground/status/1656330306616705026?s=20
- https://www.dragos.com/blog/deconstructing-a-cybersecurity-event/
- https://www.helpnetsecurity.com/2023/05/11/dragos-ransomware-extortion-attempt/

El Ministerio de Justicia de Japón habría sido víctima de un ciberataque

El Ministerio de Justicia de Japón ha sido víctima de un presunto ciberataque llevado a cabo por el grupo de ciberdelincuentes Anonymous, en respuesta a la política migratoria del país. Según el Ejecutivo japonés, varias páginas web del Ministerio de Justicia han sido atacadas desde la noche del lunes. El Ministerio ha declarado que está investigando el incidente para tomar las medidas necesarias.

Prioridad: 3 Importante.

Ampliar información:

- https://www.ciberseguridadlatam.com/2023/05/10/el-ministerio-de-justicia-de-japon-ha-sido-victima-de-un-presunto-ciberataque/
- https://www.lavanguardia.com/vida/20230509/8952333/ejecutivo-japones-sufre-presunto-ciberataque-anonymous-politica-migratoria.html

---

EE.UU. afirma haber desactivado Turla/Snake, la operación de ciberespionaje rusa

Altos funcionarios dijeron que los expertos técnicos del FBI identificaron y deshabilitaron el malware Turla (aka Snake y Uroburos) utilizado por el servicio de seguridad ruso FSB contra un número no revelado de computadoras estadounidenses, una medida que esperaban asestaría un golpe mortal a uno de los principales programas de espionaje cibernético de Rusia.

Prioridad: 3 Importante.

Ampliar información:

- https://attack.mitre.org/groups/G0010/
- https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled
- https://www.reuters.com/world/fbi-says-it-has-sabotaged-hacking-tool-created-by-elite-russian-spies-2023-05-09/

Los servidores en la nube son la principal vía de entrada de los ciberataques a empresas

Hoy en día, la ciberseguridad se ha convertido en un asunto prioritario para todas las empresas, independientemente de su tamaño o envergadura. La evolución de los modelos de trabajo y la generalización del teletrabajo a causa de la pandemia ha ido transformando las infraestructuras informáticas de las empresas en los últimos años, lo que ha implicado, a su vez, que se abra un abanico de posibilidades nuevas para los ciberdelincuentes, quienes están encontrando nuevos focos de atención. En este sentido, los servidores en la nube se colocan ahora en primera posición como vía de entrada de los ciberdelincuentes para el 41% de las empresas, según el Informe de Ciberpreparación 2022 de Hiscox.

Prioridad: 3 Importante.

Ampliar información:

- https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2022

Cómo usar "WinRar -df" para hacer desaparecer una organización

El grupo delictivo ruso SandWorm se ha relacionado con un ataque a las redes estatales de Ucrania donde se utilizó WinRar para destruir datos en dispositivos gubernamentales. En un nuevo aviso, el Equipo de Respuesta a Emergencias Informáticas del Gobierno de Ucrania (CERT-UA) dice que los delincuentes informáticos rusos utilizaron cuentas VPN comprometidas que no estaban protegidas con autenticación multifactor para acceder a sistemas críticos en las redes estatales de Ucrania.

Prioridad: 3 Importante.

Ampliar información:

- https://malpedia.caad.fkie.fraunhofer.de/actor/sandworm
- https://www.bleepingcomputer.com/news/security/russian-hackers-use-winrar-to-wipe-ukraine-state-agencys-data/
- https://blog.segu-info.com.ar/2023/05/como-usar-winrar-df-para-hacer.html
- https://hipertextual.com/2023/05/hackers-rusos-winrar-ataque-gobierno-ucrania